APPLICATION UNDER UNITED STATES PATENT LAWS

Atty. Dkt. No. PMS-265915
(M#)

Invention: **ENCRYPTING SECURITY DEVICE AND PROCESS**

Inventor: HOWARD STEIN

Pillsbury Madison & Sutro LLP
Attn: W. Patrick Bengtsson
50 Fremont Street
Fifth Floor (1258)
San Francisco, CA 94105-2230
Attorneys
Telephone: (415) 983-1000
Express Mail Label No.
EL492832140US

This is a:

- ☐ Provisional Application
- ☒ Regular Utility Application
- ☐ Continuing Application
- ☐ PCT National Phase Application
- ☐ Design Application
- ☐ Reissue Application
- ☐ Plant Application
- ☐ Substitute Specification
  Sub. Spec Filed _____
  in App. No. ___/_____
- ☐ Marked up Specification re
  Sub. Spec. filed _____
  In App. No ___/_____

SPECIFICATION

ENCRYPTING SECURITY DEVICE AND PROCESS

Inventor: Howard Stein

Field of the Invention

The invention relates to an encryption security device and process to limit access to an associated apparatus. The associated apparatus can comprise such diverse items as a computer, a computer program, a vehicle, a home, a safe or other devices or places to which access should be restricted. Specifically the invention relates to the use of a photograph as an aspect of an encryption security device.

Description of Related Art

User carried security devices are already known, however no currently existing security device utilizes a photograph, with its multiplicity of randomly placed picture elements.

There are other security processes, which use words or graphics as a passkey, but hackers have broken into all of these because the underlying passkey is based upon linguistics or logic.

Summary of the Invention

Described is an encrypting security device for restricting access to an associated apparatus. The security device comprises a security photograph, with a multiplicity of picture elements, which is inserted into a high-resolution scanner or equivalent. An associated apparatus can be initialized such that it recognizes the specific security photograph and will not allow access without the insertion of said security photograph into the scanner.

The security photograph necessarily comprises a plurality of picture elements. Preferably the security photograph comprises a picture which incorporates a vast number of random picture elements. One type of photograph which can advantageously be used is an enlargement of the center of a cut gemstone. Enlargements of other items of unique structure can be used equally advantageously.

Importantly, this encryption methodology, unlike existing methodologies, prevents access by hackers trying to use alphabetical and numerical replacement methodology because the program sees the picture as a whole as well as made up of a series of elements. If one element is not correct in the whole, the hacker cannot determine which of the hacker's replacements is right or wrong because the security device either prevents further attempts to pass the security test or shuts the secured device down so that further hacking is impossible.

Brief Description of the Figures

The invention will be better understood by reference to the appended figures and description.

Figure 1 illustrates a process for access to a computer using one embodiment of the described security device.

Figure 2 illustrates a process of producing one embodiment of the present invention.

Description of the Invention

The described invention, in one preferred embodiment, is a security device comprising a photograph. The photograph necessarily incorporates a multiplicity of picture elements. An apparatus such as a computer or a computer program or another apparatus requiring access which can be secured is associated with the security device. The apparatus is initialized such that a specific security photograph is required to access the apparatus or an aspect of the workings of the apparatus. In one embodiment, in order for the apparatus to be initialized the security photograph is

scanned for initialization. Henceforth the identical photograph must be scanned for access to the associated apparatus.

After the security photograph has been scanned, the security photograph is encrypted onto the computer hard disc as a program file for the purpose of blocking access to the computer. In one embodiment the computer can henceforth not be booted up without first scanning an identical security photograph. The direction given by the encryption program when the computer is turned on is to place a 'security code' (security photograph) in a high-resolution scanner so that the original photograph used to encrypt entry to the computer is compared with the security photograph being scanned. The two photographs must match exactly for the computer to become functional and allow a user to access the programs. The requirements for the two photographs to match can require a high level of detail.

This process could further be used to access individual programs or files on the hard drive of the computer. The process could also be used to protect already existing programs or files.

This is a unique process by which any user can prevent others from operating the users computer, programs and accessing data. In one embodiment the following is required for access to a computer

1) a computer

2) an attached scanner

3) a program which is initialized by the user to recognize a scan of a photograph

4) a photograph.

The process requires a program, which requires the user to insert a passkey device into the scanner, which the program will thereafter use to compare in order for any user to start the computer. Once the user has scanned the passkey device into the program the computer will not boot without the passkey device being inserted into the scanner, being recognized as the correct device by the program, and the program then allowing the computer to boot.

Figure 1 illustrates an exemplary process of using an embodiment of the described security device. In Figure 1 security photograph 10 of an enlarged gemstone is placed in high-resolution scanner 11. Scanner 11 is connected with computer 12. When security photograph 10 is initially placed in scanner 11 computer 12 is initialized to require security photograph 10 as a pass key equivalent. Thereafter the insertion of security photograph 10 in scanner 11 allows access to computer 12.

In one preferred embodiment security photograph 10 is an enlargement of a photograph of the center of a gemstone. A highly magnified interior of a gem is non-logical and a decoding device cannot use a logic based replacement program to determine what pattern the magnification of the internal structure of a gem will have unless the hacker knows exactly which gem has been used, the exact angle from which the picture of the gem was taken and the exact level of magnification used in the original passkey device.

Figure 2 illustrates the process used to obtain the security photograph in one embodiment of the invention. Camera 20 is attached to microscope 21. Camera 20 is employed to take a picture of an enlargement of the center of gemstone 22 (a cut diamond, emerald, ruby or other gem). The enlargement used can be from a 10 to 40 power, the industry standard, or from two power to infinity depending on the level of random variability desired by the user for the security photograph. The resulting picture can either be a transparency or a print. Once the security photograph has been selected, it is developed through ordinary film development processes. Magnification of gemstone 22 is required because no two gems have identical internal structure and the greater the degree of magnification the greater the unpredictable variations of such internal structure will be revealed thus making duplication of the security photograph impossible. A picture taken of the same gem using different magnification or which is taken from a different angle, no matter how minutely at variance from the original, will not be recognized by the program as the correct security photograph and the apparatus associated with the security photograph will not start.

For this embodiment of the security device a picture of the center of any polished gem could be used. Further a piece of granite could be cut into pieces and enlarged photographs of the unique structural surface of the granite could be used as a

security photograph. No two security photographs would be exactly the same.

In another preferred embodiment the security photograph could comprise a magnified photograph of any suitable object. In another embodiment the security photograph could comprise any picture which comprises a multitude of random picture elements.

The described security device can be used to secure a computer, a computer program, a vehicle of any description, a gun, a home, a cash register, a safe or any other apparatus which requires secured access.

In a preferred embodiment of the invention, the program in the security device process will allow the user several levels of security from which to choose. For example the following options could be made available:

(1) a security photograph required prior to booting of the computer;

(2) the intermittent random scanning of the security photograph by the scanner at the direction of the program for so long as the computer is booted in order for it not to shut down (i.e., if the security photograph is removed from the scanner at any time the computer will either shut down or freeze until the security photograph is re-inserted);

(3) a security photograph, or one or more different security photographs required for the user to use or continue to use different programs or data in the computer.

The described security photograph is not like any other security code because the complicated picture consists of so many thousands of randomly organized picture elements which cannot be decoded because they are in no logical order, nor do they consist of known alphabets or symbols. Even if an unauthorized user knew what the security photograph had been taken of, the security photograph could not be duplicated because the angle, distance and magnification would be different for each security photograph.